Avira AntiVir Personal – Free Antivirus

User Manual

AVIRA®

Trademarks and Copyright

Trademarks

Copyright information

Table of Contents

1 Introduction

Avira AntiVir Personal from Avira GmbH protects you computer against viruses, malware, adware and spyware, unwanted programs and other dangers. This manual deals with viruses and software in brief.

The manual describes the program installation and operation.

Please go to our website http://www.avira.com/free-av where you can download the Avira AntiVir Personal manual in PDF from, update Avira AntiVir Personal , get information on the version of Avira AntiVir Premium available for purchase .

You can also find information on our website such as telephone numbers for technical support and information on how to subscribe to our newsletter.

Your Avira GmbH team

2 Icons and emphases

The following icons are used:

Icon / Designation	**Explanation**
✓	Placed before a condition which must be fulfilled prior to implementation.
▶	Placed before an action step that you implement.
→	Placed before an event that follows the previous action.
Warning	Placed before a warning of the danger of critical data loss.
Note	Placed before a link to particularly important information or a tip which makes Avira AntiVir Personal easier to use.

The following emphases are used:

Emphasis	**Explanation**
Cursive	File name or path data.
	Displayed software interface elements (e.g. window heading, window field or options box).
Bold	Clicked software interface elements (e.g. menu item, section or button)

3 Product information

This chapter contains all information relevant to the purchase and use ofAvira AntiVir Personal:

- see chapter: Delivery scope
- see chapter: System requirements
- see chapter: Licensing

Avira AntiVir Personal is a comprehensive and flexible tool you can rely on to protect your computer from viruses, malware, unwanted programs, and other dangers

▶ Please note the following information:

Note
Loss of valuable data usually has dramatic consequences. Even the best virus protection program cannot provide one hundred percent protection from data loss. Make regular copies (Backups) of your data for security purposes.

Note
A program can only provide reliable and effective protection from viruses, malware, unwanted programs and other dangers if it is up-to-date. Make sure Avira AntiVir Personal is up-to-date with automatic updates. Configure the program accordingly.

3.1 Delivery scope

Avira AntiVir Personal gives you the following functions:

- Control Center for monitoring, administering and controlling the entire program
- Central configuration with user-friendly standard and advanced options and context-sensitive help
- Scanner (On-Demand Scan) with profile-controlled and configurable scan for all known types of virus and malware
- Integration into the Windows Vista User Account Control allows you to carry out tasks requiring administrator rights
- Guard (On-Access Scan) for continuous monitoring of all file access attempts
- Integrated quarantine management to isolate and process suspicious files
- Rootkit protection for detecting hidden malware installed in your computer system (rootkits)
  (Not available under Windows XP 64 bit)
- Direct access to detailed information on the detected viruses and malware via the Internet
- Simple and quick updates to the program, virus definitions, and search engine through Single File Update and incremental VDF updates via a web server on the Internet
- Integrated Scheduler for planning one-off or recurring jobs such as updates or scans

- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method
- Detection of all conventional archive types including detection of nested archives and smart extension detection
- High-performance multithreading function (simultaneous high-speed scanning of multiple files)

3.2 System requirements

For Avira AntiVir Personal to work perfectly, the computer system must fulfill the following requirements:

- Computer as from Pentium, at least 266 MHz
- Operating system
- Windows 2000, SP4 and update rollup 1 or
- Windows XP, SP2 (32 or 64 Bit) or
- Windows Vista (32 or 64 Bit, SP 1 recommended)
- Windows 7 (32 or 64 Bit)
- At least 100 MB of free hard disk memory space (more if using Quarantine for temporary storage)
- At least 192 MB RAM under Windows 2000/XP
- At least 512 MB RAM under Windows Vista
- For the installation of Avira AntiVir Personal: Administrator rights
- For all installations: Windows Internet Explorer 6.0 or higher
- Internet connection where appropriate (see Installation)

Information for Windows Vista users

On Windows 2000 and Windows XP, many users work with administrator rights. However, this is not desirable from the point of view of security, because it is then easy for viruses and unwanted programs to infiltrate computers.

For this reason, Microsoft is introducing the "User Account Control" with Windows Vista. This offers more protection for users who are logged in as administrators: thus in Windows Vista, one administrator only has the privileges of a normal user at first. Actions for which administrator rights are required are clearly marked in Windows Vista with an information icon. In addition, the user must explicitly confirm the required action. Privileges are only increased and the administrative task carried out by the operating system after this permission has been obtained.

Avira AntiVir Personal requires administrator rights for some actions in Windows Vista. These actions are marked with the following symbol: 🛡. If this symbol also appears on a button, administrator rights are required to carry out this action. If your current user account does not have administrator rights, the Windows Vista dialog of the User Account Control asks you to enter the administrator password. If you do not have an administrator password, you cannot carry out this action.

3.3 Licensing and Upgrade

In order to be able to use Avira AntiVir Personal, you require a license. You thereby accept the license conditions of Avira AntiVir Personal.

The license is provided in the form of an activation key. The activation key is a letter and figure code which you will receive after purchasing Avira AntiVir Personal . The activation key contains the exact data of your license, i.e. which programs have been licensed for which period of time.

The activation key will be sent to you by email, if you have purchased AntiVir Personal on the Internet or it is rendered on the product packaging.

In order to license your program, please enter your activation key to activate Avira AntiVir Personal. The product activation may be carried out during installation. However, you can also activate Avira AntiVir Personal after the installation in License Manager, under Help::License management .

A valid activation key is already contained in Avira AntiVir Personal. For this reason, product activation is not required.

In License Manager, you have the option of launching an upgrade for a product from the AntiVir desktop product family. Manual uninstallation of the old product and manual installation of the new product is not required. When upgrading from License Manager, you enter the activation code for the product you want to upgrade in the License Manager input box. The new product is automatically installed.

The following product upgrades can be executed automatically via License Manager:

- Upgrade of Avira AntiVir Personal to Avira AntiVir Premium
- Upgrade of Avira AntiVir Personal to Avira Premium Security Suite
- Upgrade of Avira AntiVir Premium to Avira Premium Security Suite

4 Installation and uninstallation

This chapter contains information relating to the installation and uninstallation of your Avira AntiVir Personal:

– see Chapter Installation: Conditions, Installation types, Install

– see Chapter Installation modules

– see Chapter Modification installation

– see Chapter Uninstallation: Uninstall

4.1 Installation

Before installing Avira AntiVir Personal, check whether your computer fulfils all the minimum system requirements. If your computer satisfies all requirements, you can install Avira AntiVir Personal.

Note
From Windows XP, Avira AntiVir Personal generates a restore point of your computer before installation of Avira AntiVir Personal. This enables you to safely remove Avira AntiVir Personal if installation fails. Note that for this the option **Turn off System Restore** under: "Start | Settings | Control Panel | System | Tab System Restore" must not be marked.
If you want to recover your system earlier, you can do so with the function "Start | Programs | Accessories | System Tools | System Restore". The restore point generated by Avira AntiVir Personal is indicated by the entry AntiVir Personal.

Installation types

During installation you can select a setup type in the installation wizard:

Express

– Not all program components are installed. The following components are not installed:

AntiVir ProActiv

AntiVir Firewall

– The program files are installed into a given standard folder under `C:\Program Files`.

– AntiVir Personal is installed with default settings. You have the option of defining custom settings using the configuration wizard.

User-defined

– You can choose to install individual program components (see Chapter Installation and uninstallation::Installation modules).

– A target folder can be selected for the program files to be installed.

– You can disable Create a desktop icon and program group in the Start menu.

- Using the configuration wizard, you can define custom settings for AntiVir Personal and initiate a short system scan which is carried out automatically after installation.

Before starting installation

- Close your email program. It is also recommended to end all running applications.
- Make sure that no other virus protection solutions are installed. The automatic protection functions of various security solutions may interfere with each other.
- Establish an Internet connection: The Internet connection is necessary for performing the following installation steps:
- Downloading the current program file and search engine, and the latest virus definition files via the installation program (for internet-based installation)
- Registering as a Avira AntiVir Personal user
- Where appropriate, carrying out a AntiVir Personal update after completed installation
- Have the license key for AntiVir Personal ready, if you want to activate AntiVir Personal.

Note

Internet-based installation:

Avira GmbH provides an installation program for the internet-based installation of Avira AntiVir Personal, which loads the current program file prior to installation by the Avira GmbH web servers. This process ensures that AntiVir Personal is installed with the latest virus definition file.

Installation with an installation package:

The installation package contains both the installation program and all necessary program files. No language selection for AntiVir Personal is available for installation with an installation package. We recommend that you carry out an update of the virus definition file after installation.

Note

For registration, Avira AntiVir Personal uses the HTTP protocol and Port 80 (web communication), as well as encryption protocol SSL and port 443, to communicate with the servers of Avira GmbH. If you are using a firewall, please ensure that the required connections and/or incoming or outgoing data are not blocked by the firewall.

Install

The installation program runs in self-explanatory dialog mode. Every window contains a certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions:

- **OK:** Confirm action.
- **Abort:** Abort action.
- **Next:** Go to next step.
- **Back:** Go to previous step.

How to install AntiVir Personal:

- Start the installation program by double-clicking on the installation file you have downloaded from the Internet or insert the program CD.

Internet-based installation

→ The dialog box *Welcome...* appears.

▶ Click **Next** to continue with the installation.

→ The dialog box *Language selection* appears.

▶ Select the language you want to use to install AntiVir Personal and confirm your language selection by clicking **Next**.

→ The dialog box *Download* appears. All files necessary for installation are downloaded by the Avira GmbH web servers. The *Download* window closes after conclusion of the download.

Installation with an installation package

→ The installation wizard opens with the dialog box *Avira AntiVir Personal*.

▶ Click *Accept* to begin the installation.

→ The installation file is extracted. The installation routine is started.

→ The dialog box *Welcome...* appears.

▶ Click **Next**.

Continuing internet-based installation and installation with an installation package

→ The dialog box with the license agreement appears.

▶ Confirm that you accept the license agreement and click **Continue**.

→ The dialog box *Private use* appears.

▶ Confirm that AntiVir Personal will be used exclusively for private purposes and not for commercial purposes and click **Continue**.

→ The dialog box *Generate serial number* appears.

▶ Where appropriate, confirm that a random serial number has been generated and transmitted during update, and click **Continue**.

→ The dialog box *Select installation type* appears.

▶ Decide whether you want to perform an express installation or a user-defined installation.

▶ Enable the option **Express** or**User-defined** and confirm by clicking **Continue**.

User-defined installation

→ The dialog box *Select destination directory* appears.

▶ Confirm the specified destination directory by clicking **Continue**.

- OR -

Use the **Browse** button to select a different destination directory and confirm by clicking **Next**.

→ The dialog box *Install components* appears:

▶ Enable or disable the required components and confirm by clicking **Continue**.

→ In the following dialog box you can decide whether to create a desktop shortcut and/or a program group in the Start menu.

▶ Click **Next**.

Resume: Express installation und user-defined installation

➜ The license wizard is opened.

In the license wizard you have the possibility of registering as a customer of AntiVir Personal and of subscribing to the Avira GmbH Newsletter. Your personal data are required for this purpose.

▶ If and when necessary, enter your data and acknowledge by clicking **Next**.

➜ In case of a registration, the following dialog box will display the result of the activation.

➜ Click **Next**.

➜ The program features will be installed. Installation progress is displayed in the dialog box.

➜ In the following dialog box you can choose whether to open the Readme file after installation is completed and whether to restart your computer.

▶ Agree where appropriate and complete the installation by clicking *Finish*.

➜ The installation wizard is closed.

Resume: User-defined installation
Configuration wizard

➜ If you choose user-defined installation, the following step opens the configuration wizard. The configuration wizard enables you to define custom settings for AntiVir Personal.

▶ Click **Next** in the welcome window of the configuration wizard to begin configuration of AntiVir Personal.

➜ The *Configure AHeAD* dialog box enables you to select a detection level for the AHeAD technology. The detection level selected is used for the Scanner (On-demand scan) and Guard (On-access scan) AHeAD technology settings.

▶ Select a detection level and continue the installation by clicking **Next**.

➜ In the following dialog box *Select extended threat categories*, you can adapt the protective functions of AntiVir Personal to the threat categories specified.

▶ Where appropriate, activate further threat categories and continue the installation by clicking *Next*.

➜ If you have selected the AntiVir Guard installation module, the*Guard start mode* dialog box appears. You can stipulate the Guard start time. At each computer reboot, the Guard will be started in the start mode specified.

Note
The specified Guard start mode is saved in the registry and cannot be changed via the Configuration.

▶ Enable the required option and continue the configuration by clicking *Next*.

➜ In the following dialog box, *System scan*, a short system scan can be enabled or disabled. The short system scan is carried out after the configuration has been completed and before the computer is rebooted, and scans running programs and the most important system files for viruses and malware.

▶ Enable or disable the *Short system scan* option and continue the configuration by clicking *Next*.

➜ In the following dialog box, you can complete the configuration by clicking *Finish*

▶ Click *Finish* to complete the configuration.

➜ The specified and selected settings are accepted.

→ If you have enabled the *Short system scan* option, the Luke Filewalker window opens. The Scanner performs a short system scan.

Resume: Express installation und user-defined installation

→ If you selected the **Restart computer** option in the final installation wizard, the computer reboots.

→ After the computer restart, the AntiVir Personal Readme file is displayed, if you selected the **Show Readme.txt** option in the installation wizard.

After a successful installation, we recommend that you check AntiVir Personal is up-to-date in the Control Center under *Overview :: Status*.

▶ Where appropriate, update AntiVir Personal to ensure the virus definition file is up-to-date.

▶ Then perform a full system scan.

4.2 Modification installation

You have the option of adding or removing individual program components of the current Avira AntiVir Personal installation (see ChapterInstallation and uninstallation::Installation modules)

If you wish to add or remove modules of the actual Avira AntiVir Personal installation, you can use the option **Add or Remove Programs** in the **Windows control panel** to **Change/Remove** programs.

Select Avira AntiVir Personal and click **Change**. In the welcome dialog of Avira AntiVir Personal select the option **Modify**. You will be guided through the installation changes.

4.3 Installation modules

In a user-defined installation or a modification installation, the following installation modules can be selected, added or removed.

- **AntiVir Personal**
  This module contains all components required for successful installation of Avira AntiVir Personal.
- **AntiVir Guard**
  The AntiVir Guard runs in the background. It monitors and repairs, if possible, files during operations such as open, write and copy in on-access mode. Whenever a user carries out a file operation (e.g. load document, execute, copy), Avira AntiVir Personal automatically scans the file. Renaming a file does not trigger a scan by AntiVir Guard.
- ***AntiVir Rootkit Protection***
  AntiVir Rootkit Protection checks whether software is already installed on your computer that can no longer be detected with conventional methods of malware protection after penetrating the computer system.

- **Shell Extension**
  The Avira AntiVir Personal Shell Extension generates an entry in the context menu of the Windows Explorer (right-hand mouse button). Scan selected files with AntiVir. With this entry you can directly scan files or directories.

4.4 Uninstallation

If you wish to remove Avira AntiVir Personal from your computer, you can use the option **Add or Remove Programs** to **Change/Remove** programs in the Windows Control Panel.

To uninstall Avira AntiVir Personal (e.g. in Windows XP and Windows Vista):

▶ Open the **Control Panel** via the Windows **Start** menu.

▶ Double click on **Programs** (Windows XP: **Software**).

▶ Select **Avira AntiVir Personal** and click**Remove**.

→ You will be asked if you really want to remove the program.

→ All components of the program are removed.

▶ Click on **Finish** to complete uninstallation.

→ Where appropriate, a dialog box appears recommending that your computer be restarted.

→ Avira AntiVir Personal is uninstalled, and all directories, files and registry entries for Avira AntiVir Personal are deleted when your computer is restarted.

5 Overview of AntiVir Personal

This chapter contains an overview of the functionality and operation of AntiVir Personal.

- see Chapter Interface and operation
- see ChapterHow to...?

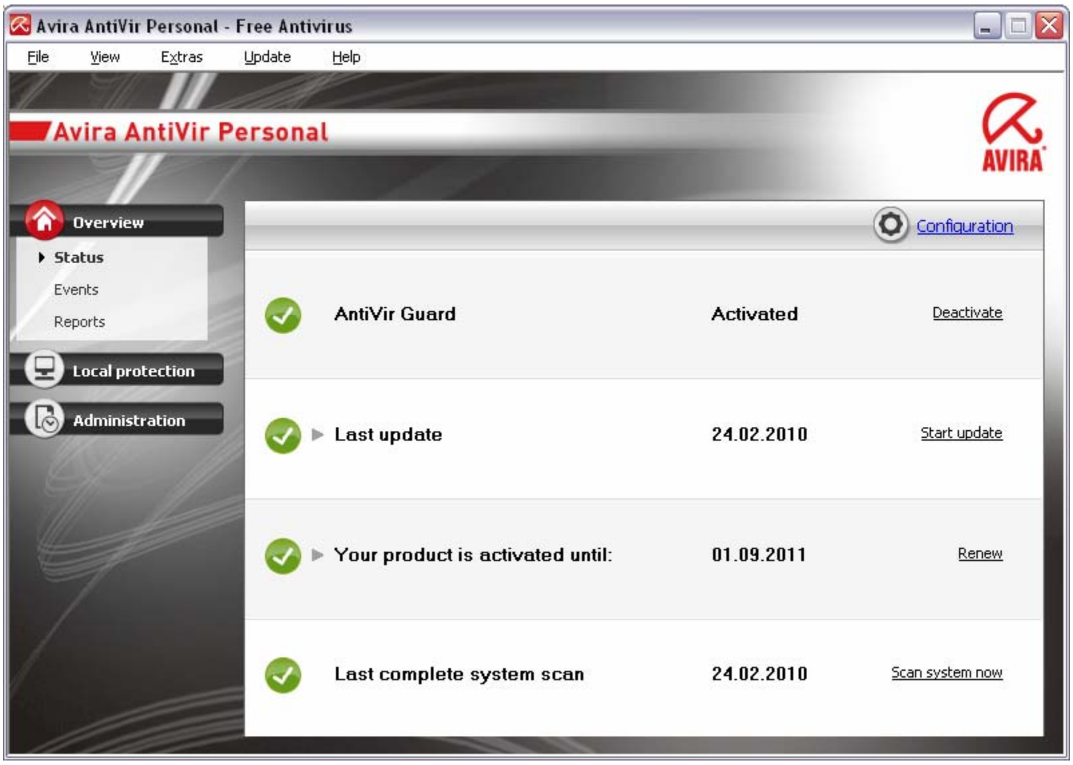
5.1 User interface and operation

Your operate AntiVir Personal via three program interface elements:

- Control Center: Monitoring and control of AntiVir Personal
- Configuration: Configuration of AntiVir Personal
- Tray Icon in the system tray of the taskbar: Open the Control Centre and other functions

5.1.1 Control Center

The Control Center is designed to monitor the protection status of your computer systems and control and operate the protection components and functions of AntiVir Personal.



AntiVir Guard	Activated	Deactivate
Last update	24.02.2010	Start update
Your product is activated until:	01.09.2011	Renew
Last complete system scan	24.02.2010	Scan system now

The Control Center window is divided into three areas: the**menu bar**, the**navigation bar** and the detail window**view**:

- **Menu bar:** In the Control Center menu bar, you can access general program functions and information on AntiVir Personal.

- **Navigation area:** In the navigation area, you can easily swap between the individual sections of the Control Center. The individual sections contain information and functions of the program components of AntiVir Personal and are arranged in the navigation bar according to activity. Example: Activity *Overview* - Section**Status**.
- **View:** This window shows the section selected in the navigation area. Depending on the section, you will find buttons to execute functions and actions in the upper bar of the detail window. Data or data objects are displayed in lists in the individual sections. You can sort the lists by clicking in the box defining how you wish to sort the list.

Starting and closing of Control Center

To start the Control Center the following options are available:

- Double-click the program icon on your desktop
- via the AntiVir Personal program entry in the start menu | program.
- via the Avira AntiVir Personal tray icon.

Close the Control Center via the menu command **Close** in the menu **File** or by clicking on the close tab in the Control Center.

Operate Control Center

To navigate in the Control Center

▶ Select an activity in the navigation bar.

→ The activity opens and other sections appear. The first section of the activity is selected and displayed in the view.

▶ If necessary, click another section to display this in the detail window.

- OR -

▶ Select a section via the menu *View*.

Note
You can activate the keyboard navigation in the menu bar with the help of the [ALT] key. If navigation is activated, you can move within the menu with the arrow keys. With the Return key you activate the active menu item.
To open or close menus in the Control Center, or to navigate within the menus, you can also use the following key combinations: [Alt] + underlined letter in the menu or menu command. Hold down the [Alt] key if you want to access a menu, a menu command or a submenu.

To process data or objects displayed in the detail window:

▶ highlight the data or object you wish to edit.

To highlight multiple elements (elements in columns), hold down the control key or the shift key while selecting the elements.

▶ Click the appropriate button in the upper bar of the detail window to edit the object

Control Center overview

- **Overview**: In **Overview** you will find all sections with which you can monitor the functioning of Avira AntiVir Personal.

- The **Status** section lets you see at a glance which Avira AntiVir Personal modules are active and provides information on the last update carried out. You can also see whether you own a valid license.
- The Events section enables you to view events generated by certain Avira AntiVir Personal modules.
- Die Reports section enables you to view the results of actions executed by Avira AntiVir Personal.

– **Local protection**: In**Local protection** you will find the components for checking the files on your computer system for viruses and malware.

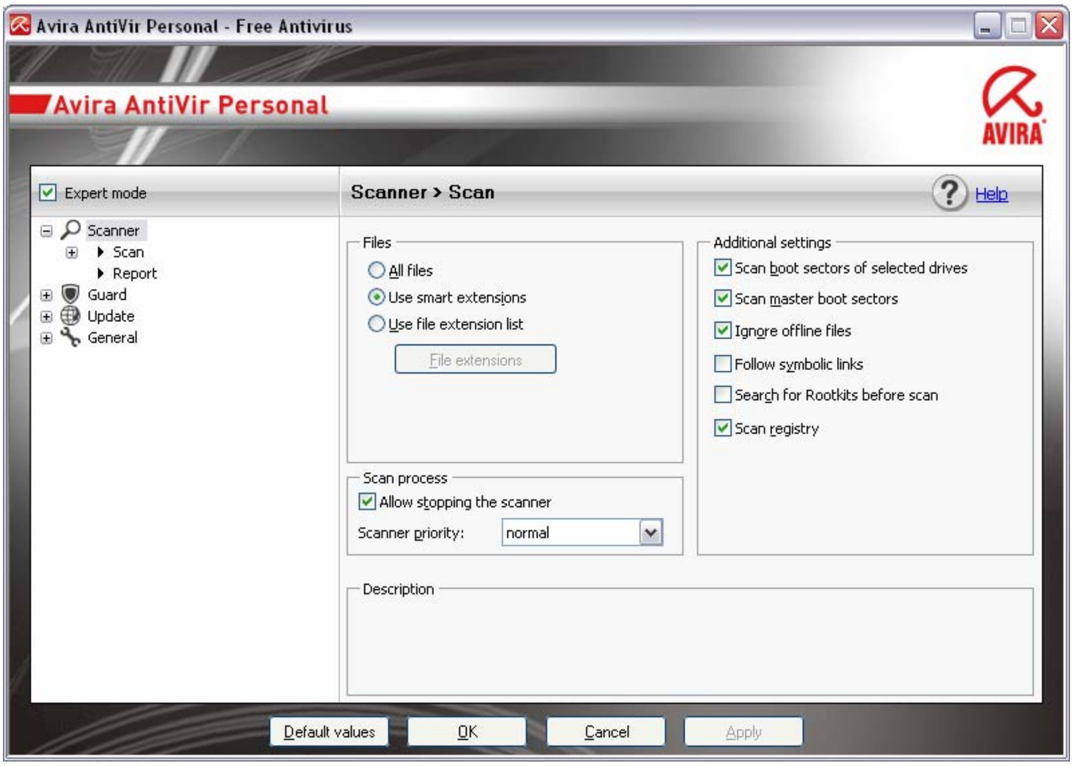
- The Scan section enables you to easily configure and start an on-demand scan. Predefined profiles enable you to run a scan with preset default options. In the same way it is possible to adapt the scan for viruses and unwanted programs to your personal requirements with the help of manual selection (not saved).
- The Guard section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".

– **Administration**: In **Administration** you will find tools for isolating and managing suspicious or infected files, and for planning recurring tasks.

- The Quarantine section contains the so-called Quarantine Manager. This is the central point for files already placed in quarantine or for suspect files which you would like to place in quarantine. It is also possible to send a selected file to the Avira Malware Research Center by email.
- The Scheduler section enables you to configure scheduled scanning and update jobs and to adapt or delete existing jobs.

5.1.2 Configuration

You can define AntiVir Personal settings in the Configuration. After installation, AntiVir Personal is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for AntiVir Personal may mean you need to adapt the protective components of AntiVir Personal.



☑ Expert mode

Scanner > Scan

Files
○ All files
● Use smart extensions
○ Use file extension list

Additional settings
☑ Scan boot sectors of selected drives
☑ Scan master boot sectors
☑ Ignore offline files
☐ Follow symbolic links
☐ Search for Rootkits before scan
☑ Scan registry

Scan process
☑ Allow stopping the scanner
Scanner priority: normal

Description

The Configuration opens a dialog box: You can save your configuration settings via the OK or Accept buttons, delete you settings by clicking the Cancel button, or restore your default configuration settings using the Restore defaults button. You can select individual configuration sections in the left-hand navigation bar.

Accessing the AntiVir Personal Configuration

You have several options for accessing the configuration:

- via the Windows control panel.
- via the Windows Security Center - from Windows XP Service Pack 2.
- via the Avira AntiVir Personal tray icon.
- in the Avira AntiVir Personal Control Center via the menu item Extras | Configuration.
- in the Avira AntiVir Personal Control Center via the Configuration button.

Note
If you are accessing configuration via the **Configuration** button in the Control Center, go to the Configuration register of the section which is active in the Control Center. Expert mode must be activated to select individual configuration registers. In this case, a dialog appears asking you to activate expert mode.

Configuration operation

Navigate in the configuration window as you would in Windows Explorer:

- Click on an entry in the tree structure to display this configuration section in the detail window
- Click on the plus symbol in front of an entry to expand the configuration section and display configuration subsections in the tree structure.

- ▶ To hide configuration subsections, click on the minus symbol in front of the expanded configuration section.

Note
To enable or disable Configuration options and use the buttons, you can also use the following key combinations: [Alt] + underlined letter in the option name or button description.

Note
All configuration sections are only displayed in expert mode. Activate expert mode to view all configuration sections. Expert mode can be protected by a password which must be defined during activation.

If you want to confirm your Configuration settings:

▶ Click **OK**.

→ The configuration window is closed and the settings are accepted.

- OR -

▶ Click **Accept**.

→ The settings are accepted. The configuration window remains open.

If you want to finish configuration without confirming your settings:

▶ Click **Cancel**.

→ The configuration window is closed and the settings are discarded.

If you want to restore all configuration settings to default values:

▶ Click **Restore defaults**.

→ All settings of the configuration are restored to default values. All amendments and custom entries are lost when default settings are restored.

Overview of configuration options

The following configuration options are available:

– **Scanner**: Configuration of on-demand scan

Scan options

Action on detections

File scan options

On-demand scan exceptions

On-demand scan heuristics

Report function setting

– **Guard**: Configuration of on-access scan

Scan options

Action on detections

On-access scan exceptions

On-access scan heuristics

Report function setting

– **General**:

Configuration of email using SMTP

Extended risk categories for on-demand and on-access scan

Security: Update status display, full system scan status display, product protection

WMI: Enable WMI support

Event log configuration

Configuration of report functions

Setting of directories used

Update: Configuration of connection to download server, set-up of product updates

Configuration of acoustic alerts when malware is detected

5.1.3 Tray icon

After installation, you will see the AntiVir Personal tray icon in the system tray of the taskbar:

Icon	Description
	AntiVir Guard is enabled
	AntiVir Guard is disabled

The tray icon displays the status of the AntiVir Guard service.

Central functions of Avira AntiVir Personal can be quickly accessed via the context menu of the tray icon. To open the context menu, click on the tray icon with the right-hand mouse button.

Entries in the context menu

- **Activate AntiVir Guard**: Enables or disables Avira AntiVir Guard.
- **Start AntiVir**: Opens the Avira AntiVir Personal Control Center.
- **Configure AntiVir**: Opens the Configuration
- **Start update** Starts an update.
- **Help**: opens this online help.
- **Avira on the Internet**: Opens the web portal of AntiVir Personal on the internet. The condition for this is that you have an active connection to the Internet.

5.2 How to...?

5.2.1 Avira AntiVir Personal automatic update

To create a job with the AntiVir Scheduler to update Avira AntiVir Personal automatically:

▶ In the Control Center, select the **Management :: Scheduler** section.

▶ Click on the *Create new job with the wizard* icon.

→ The dialog box *Name and description of job* appears.

▶ Give the job a name and, where appropriate, a description.

→ The dialog box *Type of job* is displayed.

▶ Select **Update job** from the list.

→ The dialog box *Time of job* appears.

▶ Select a time for the update:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**

Note
We recommend that you update Avira AntiVir Personal regularly and often. The recommended update interval is: 24 hours.

▶ Where appropriate, specify a date according to the selection.

▶ Where appropriate, select additional options (availability depends on type of job):

- **Repeat job if the time has already expired**

  Past jobs are carried out that could not be carried out at the required time, for example because the computer was switched off.

→ The dialog box *Select display mode* appears.

▶ Select the display mode of the job window:

- **Minimize**: progress bar only
- **Maximize**: Entire job window
- **Hide**: No job window

▶ Click **Finish**.

→ Your newly created job appears on the home page of the **Administration :: Scan** section as activated (check mark).

▶ Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:

View properties of a job

Modify job

Delete job

Start job

Stop job

5.2.2 Start a manual update

You have various options for starting an Avira AntiVir Personal update manually: When an update is started manually, the virus definition file and search engine are always updated. A product update can only take place if you have activated the option **Download and automatically install product updates** in the configuration under General :: Update

To start an Avira AntiVir Personal update manually:

▶ With the right-hand mouse button, click on the Avira AntiVir Personal tray icon in the taskbar.

→ A context menu appears.

▶ Select **Start update**.

→ The *Updater* dialog box appears.

- OR -

▶ In the Control Center, select the section **Overview :: Status**.

▶ In the *Last update* field, click on the **Start update** link.

→ The Updater dialog box appears.

- OR -

▶ In the Control Center, in the **Update** menu, select the menu command *Start update*.

→ The Updater dialog box appears.

Note
We strongly recommend regular automatic updates for Avira AntiVir Personal. The recommended update interval is: 24 hours.

Note
You can also carry out a manual update directly via the Windows security centre.

5.2.3 On-demand scan: Using a scan profile to scan for viruses and malware

A scan profile is a set of drives and directories to be scanned.

The following options are available for scanning via a scan profile:

– Use predefined scan profile

if the predefined scan profile corresponds to your requirements.

– Customize and apply scan profile (manual selection)

if you want to scan with a customized scan profile.

Depending on the operating system, various icons are available for starting a scan profile:

– In Windows XP and 2000:

🔍 This icon starts the scan via a scan profile.

– In Windows Vista:

In Microsoft Windows Vista, the control center at the moment only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the control centre with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

🔍 This icon starts a limited scan via a scan profile. Only directories and files that Windows Vista has granted access rights to are scanned.

🔍 This icon starts the scan with extended administrator rights. After confirmation, all directories and files in the selected scan profile are scanned.

To scan for viruses and malware with a scan profile:

- Go to Control Center and select the section **Local protection :: Scan**.

→ Predefined scan profiles appear.

- Select one of the predefined scan profiles.

  -OR-

- Adapt the scan profile *Manual selection*.
- Click on the icon (Windows XP: 🔍 or Windows Vista: 🔍).
- The *Luke Filewalker* window appears and an on-demand scan is started.

→ When the scan is completed, the results are displayed.

If you want to adapt a scan profile:

- In the scan profile, expand **Manual Selection** the file tree so that all the drives you want to scan are open:
- Highlight the nodes you want to scan by clicking on the box:

5.2.4 On-demand scan: Scan for viruses and malware using Dragamp;Drop

To scan for viruses and malware systematically using Drag&Drop:

✓ The Avira AntiVir Personal Control Center has been opened.

- Highlight the file
- Use the left-hand mouse button to drag the highlighted file into the *Control Center*.

→ The *Luke Filewalker* window appears and an on-demand scan is started.

→ When the scan is completed, the results are displayed.

5.2.5 On-demand scan: Scan for viruses and malware via the context menu

To scan for viruses and malware systematically via the context menu:

- Click with the right-hand mouse button (e.g. in Windows Explorer, on the desktop or in an open Windows directory) on the file

→ The Windows Explorer context menu appears.

▶ Select **Scan selected files with AntiVir** in the context menu.

→ The *Luke Filewalker* window appears and an on-demand scan is started.

→ When the scan is completed, the results are displayed.

5.2.6 On-demand scan: Automatically scan for viruses and malware

Note
After installation, the scan job *Full system scan* is created in the Scheduler: A full system scan is automatically carried out at a recommended interval.

To create a job to automatically scan for viruses and malware:

▶ In the Control Center, select the **Management :: Scheduler** section.

▶ Click on the icon

→ The dialog box *Name and description of job* appears.

▶ Give the job a name and, where appropriate, a description.

→ The dialog box *Type of job* appears.

▶ Select **Scan job**.

→ The dialog box *Select profile* appears.

▶ Select the profile to be scanned.

→ The dialog box *Time of job* appears.

▶ Select a time for the scan:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**

▶ Where appropriate, specify a date according to the selection.

▶ Where appropriate, select the following additional options (availability depends on job type):

- **Repeat job if the time has already expired**

  Past jobs are carried out that could not be carried out at the required time, for example because the computer was switched off.

→ The dialog box *Select display mode* appears.

▶ Select the display mode of the job window:

- **Minimize**: progress bar only
- **Maximize**: Entire job window
- **Hide**: No job window

- Select the *Shut down computer* option if you want the computer to shut down automatically when the scan is finished. This option is only available if the display mode is set to minimized or maximized.
- Click **Finish**.

→ Your newly created order appears as activated (check mark) on the homepage of the section *Administration :: Scheduler*.

- Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:

View properties of a job

Modify job

Delete job

Start job

Stop job

5.2.7 On-demand scan: Targeted scan for active rootkits

To scan for active rootkits, use the predefined scan profile *Scan for rootkits*.

To scan for active rootkits systematically:

- Go to Control Center and select the section **Local protection :: Scan**.

→ Predefined scan profiles appear.

- Select the predefined scan profile **Scan for active malware**.
- Where appropriate, highlight other nodes and directories to be scanned by clicking on the check box of the directory level.
- Click on the icon (Windows XP: 🔍 or Windows Vista: 🔍).

→ The *Luke Filewalker* window appears and an on-demand scan is started.

→ When the scan is completed, the results are displayed.

5.2.8 Reacting to detected viruses and malware

For the individual protection components of AntiVir Personal, you can define how AntiVir Personal reacts to a detected virus or unwanted program in the Configuration under the section *Action for concerning files*.

There are no configurable action options with the Guard component. When a virus or unwanted program is detected, you will receive a desktop notification. In the desktop notification you can remove the detected malware or forward the malware using the Details button to the Scanner component for further virus management. The Scanner opens a window containing notification of the detection, which gives you various options for managing the affected file via a context menu (see Detection::Scanner):

Action options for the Scanner:

- **Interactive**

  In interactive action mode, the results of the Scanner scan are displayed in a dialog box. This option is enabled as the default setting.
  In the case of **Scanner scan**, you will receive an alert with a list of the affected files when the scan is complete. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the Scanner.

- **Automatic**

  In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically.

Action options for :

- **Interactive**

  In interactive action mode, if a virus or unwanted program is detected, a dialog box appears in which you can select what to do with the infected object. This option is enabled as the default setting.

- **Automatic**

  In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically.

In interactive action mode, you can react to detected viruses and unwanted programs by selecting an action for the infected object, displayed in the alert, and executing the selected action by clicking Confirm.

The following actions for handling infected objects are available for selection:

Note
Which actions are available for selection depends on the operating system, the protection components (AntiVir Guard, AntiVir Scanner) reporting the detection, and the type of malware detected.

Actions of the Scannerand the Guard:

- **Repair**

  The file is repaired

  This option is only available if the infected file can be repaired.

- **Move to quarantine**

  The file is packaged into a special format (**.qua*) and moved to the Quarantine directory *INFECTED* on your hard disk, so that direct access is no longer possible. Files in this directory can be repaired in Quarantine at a later data or, if necessary, sent to Avira GmbH.

- **Delete**

  The file will be deleted. If a boot sector virus is detected, this can be deleted by deleting the boot sector. A new boot sector is written.

- **Rename**

  The file is renamed with a **.vir* extension. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can be repaired and given their original name at a later time.

- **Ignore**

Avira AntiVir Personal takes no further action. The infected file remains active on your computer.

Warning
This could result in loss of data and damage to the operating system! Only select the *Ignore* option in exceptional cases.

– **Deny access**

Action option for Guard detections: Access to the infected file is blocked. The detection is only entered in the report file if the report function is enabled).

– **Copy to quarantine**

Action option for a rootkit detection: The detection is copied in quarantine.

– **Repair boot sector | Download repair tool**

Action options when infected boot sectors are detected: AntiVir Personal contains a number of options for repairing infected diskette drives. If AntiVir Personal is unable to perform the repair, you can download a special tool for detecting and removing boot sector viruses.

Note
If you carry out actions on running processes, the processes in question are terminated before the actions are carried out.

Note
We recommend that you move any suspicious file that cannot be repaired to Quarantine.

5.2.9 Quarantine: Handling quarantined files (*.qua)

To handle quarantined files:

▶ In the Control Center, select the section **Administration :: Quarantine**.

▶ Check which files are involved, so that, if necessary, you can reload the original back onto your computer from another location.

If you want to see more information on a file:

▶ Highlight the file and click on ⓘ

→ The dialog box *Properties* appears with more information on the file.

If you want to rescan a file:

Scanning a file is recommended if the Avira AntiVir Personal virus definition file has been updated and a false positive report is suspected. This enables you to confirm a false positive with a rescan and restore the file.

▶ Highlight the file and click on 🔍

→ The file is scanned for viruses and malware using the on-demand scan settings.

→ After the scan, the dialog *Scan statistics* appears which displays statistics on the status of the file before and after the rescan.

To delete a file:

▶ Highlight the file and click on ☒ .

If you want to upload the file to a Avira Malware Research Center web server for analysis:

- Highlight the file you want to upload.
- Click on

→ A dialog opens with a form for inputting your contact data.

- Enter all the required data.
- Select a type: **Suspicious file** or **False positive**.
- Click **OK.**

→ The file is uploaded to a Avira Malware Research Center web server in compressed form.

Note
In the following cases, analysis by the Avira Malware Research Center is recommended:
Heuristic hits (Suspicious file): During a scan, a file has been classified as suspicious by AntiVir Personal and moved to quarantine: Analysis of the file by the Avira Malware Research Center has been recommended in the virus detection dialog box or in the report file generated by the scan.

Note
The size of the files you upload is limited to 20 MB uncompressed or 8 MB compressed.

Note
You can only upload one file at a time.

If you want to export the properties of a quarantined object in a text file:

- Highlight the quarantined object and click on

→ A text file opens containing the data from the selected quarantined object.

- Save the text file.

You can also restore the files in Quarantine:

– see Chapter: Quarantine: Restoring files in quarantine

5.2.10 Quarantine: Restore the files in quarantine

Different icons control the restore procedure, depending on the operating system:

– In Windows XP and 2000:

This icon restores the files to their original directory.

This icon restores the files to a directory of your choice.

– In Windows Vista:

In Microsoft Windows Vista, the control center at the moment only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the control centre with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

This icon restores the files to a directory of your choice.

This icon restores the files to their original directory. If extended administrator rights are necessary to access this directory, a corresponding request appears.

To restore files in quarantine:

Warning
This could result in loss of data and damage to the operating system of the computer! Only use the function *Restore selected object* in exceptional cases. Only restore files that could be repaired by a new scan.

✓ File rescanned and repaired.

▶ In the Control Center, select the section **Administration :: Quarantine**.

Note

Emails and email attachments can only be restored using the option and if they have the extension **.eml*.

To restore a file to its original location:

▶ Highlight the file and click on the (Windows 2000/XP: , Windows Vista). This option is not available for emails.

Note

Emails and email attachments can only be restored using the option and if they have the extension **.eml*.

→ A message appears asking if you want to restore the file.

▶ Click **Yes**.

→ The file is restored to the directory it was in before it was moved to quarantine.

To restore a file to a specified directory:

▶ Highlight the file and click on . .

→ A message appears asking if you want to restore the file.

▶ Click **Yes**.

→ The Windows default window for selecting the directory appears.

▶ Select the directory to restore the file to and confirm.

→ The file is restored to the selected directory.

5.2.11 Quarantine: move suspicious files to quarantine

To move a suspect file to quarantine manually:

▶ In the Control Center, select the section **Administration :: Quarantine**.

▶ Click on . .

→ The Windows default window for selecting a file appears.

▶ Select the file and confirm.

→ The file is moved to quarantine.

You can scan files in quarantine with the AntiVir Scanner:

- see Chapter: Quarantine: Handling quarantined files (*.qua)

5.2.12 Scan profile: Amend or delete file type in a scan profile

To stipulate additional file types to be scanned or exclude specific file types from the scan in a scan profile (only possible for manual selection):

✓ In the Control Center, go to the **Local protection ::** *Scan* section.

▶ With the right-hand mouse button, click on the scan profile you want to edit.

→ A context menu appears.

▶ Select **File filter**.

▶ Expand the context menu further by clicking on the small triangle on the right-hand side of the context menu.

→ The entries *Default*, *Scan all files* and *User-defined* appear.

▶ Select **User-defined**.

→ The *File extensions* dialog box appears with a list of all file types to be scanned with the scan profile.

If you want to exclude a file type from the scan:

▶ Highlight the file type and click **Delete**.

If you want to add a file type to the scan:

▶ Highlight the file type.

▶ Click **Add** and enter the file extension of file type into the input box.

Use a maximum of 10 characters and do not enter the leading dot. Wildcards (* and ？) are allowed as replacements.

5.2.13 Scan profile: Create desktop shortcut for scan profile

You can start an on-demand scan directly from your desktop via a desktop shortcut to a scan profile without accessing the Avira AntiVir Personal Control Center.

To create a desktop shortcut to the scan profile:

✓ In the Control Center, go to the **Local protection ::** *Scan* section.

▶ Select the scan profile you want to create a shortcut for.

▶ Click on the icon

→ The desktop shortcut is created.

5.2.14 Events: Filter events

Events that have been generated by AntiVir Personal program components are displayed in the Control Center under **Overview :: Events** (analogous to the event display of your Windows operating system). The program components are:

- Updater
- Guard
- Scanner
- Scheduler

The following event types are displayed:

- Information
- Warning

- Error
- Detection

To filter displayed events:

▶ In the Control Center, select the section **Overview :: Results**.

▶ Check the box of the program components to display the events of the activated components.

- OR -

Uncheck the box of the program components to hide the events of the deactivated components.

▶ Check the event type box to display these events.

- OR -

Uncheck the event type box to hide these events.

6 Scanner::Overview

With the Scanner component, you can carry out targeted scans (on-demand scans) for viruses and unwanted programs. The following options are available for scanning for infected files:

- **On-demand scan via context menu**
  The on-demand-scan via the context menu (right-hand mouse button - entry **Scan selected files with AntiVir**) is recommended if, for example, you wish to scan individual files and directories. Another advantage is that it is not necessary to first start the Avira AntiVir Personal Control Center for an on-demand scan via the context menu.
- **On-demand scan via drag & drop**
  When a file or directory is dragged into the program window of the Avira AntiVir Personal Control Center, the Scanner scans the file or directory and all sub-directories it contains. This procedure is recommended if you wish to scan individual files and directories that you have saved, for example, on your desktop.
- On-demand scan via profiles
  This procedure is recommended if you wish to regularly scan certain directories and drives (e.g. your work directory or drives on which you regularly store new files). You do not then need to select these directories and drives again for every new scan, you simply select using the relevant profile.
- **On-demand scan via the Scheduler**
  The Scheduler enables you to carry out time-controlled scans.

Special processes are required when scanning for rootkits, boot sector viruses, and when scanning active processes. The following options are available:

- Scan for rootkits using the scan profile *Scan for active malware*
- Scan active processes via the scan profile *Active processes*
- Scan for boot sector viruses via the menu command **Scan for boot sector viruses** in the **Extras** menu

7 Updates

The effectiveness of anti-virus software depends on how up-to-date the program is, in particular the virus definition file and the search engine. To carry out updates, the Updater component is integrated into AntiVir Personal. The Updater ensures that Avira AntiVir Personal is always up-to-date and able to deal with the new viruses that appear every day. Updater updates the following components:

- Virus definition file:

  The virus definition file contains the virus patterns of the harmful programs used by AntiVir Personal to scan for viruses and malware and repair infected objects.

- Search engine:

  The search engine contains the methods used by AntiVir Personal to scan for viruses and malware.

- Program files (product update):

  Update packages for product updates make extra functions available to the individual program components.

An update checks whether the virus definition file and search engine are up-to-date and if necessary implements an update. Depending on the settings in the configuration, the Updater also carries out a product update or informs you of the product updates available. After a product update, you may have to restart your computer system. If only the virus definition file and search engine are updated, the computer does not have to be restarted.

Note
For security reasons, the Updater checks whether the Windows host file of your computer was altered to the effect that, for example, the Avira AntiVir Personal update URL was manipulated by malware and diverts the Updater to unwanted download sites. If the Windows host file has been manipulated, this is shown in the Updater report file.

AntiVir Personal is automatically updated in the following interval: 24 hours. You can edit or disable the automatic update through the configuration (Configuration::Update).

In the Control Center under Scheduler, you can create additional update jobs that are carried out by Updater at the specified intervals. You also have the option to start an update manually:

- In the Control Center: in the Update menu and in the Status section
- via the context menu of the tray icon

Updates can be obtained from the Internet via a Web server of the manufacturer. The existing network connection is the default connection to the download servers of Avira GmbH. You can modify this standard setting in the configuration under General :: Update.

8 FAQ, Tips

This chapter provides a collection of frequently asked questions (FAQs) relating to Avira AntiVir Personal, a troubleshooting section and tips and tricks for using Avira AntiVir Personal.

see Chapter Troubleshooting

see Chapter Keyboard commands

see ChapterWindows Security Center

8.1 Troubleshooting

Here you will find information on causes and solutions of possible problems.

The error message *Connection failed while downloading the file ...* appears when attempting to start an update.

Reason: Your Internet connection is inactive. This is why Avira AntiVir Personal cannot find the web server on the Internet.

▶ Test whether other Internet services such as WWW or email work. If not, reestablish the Internet connection.

Reason: The proxy server cannot be reached.

▶ Check whether the login for the proxy server has changed and adapt it to your configuration if necessary.

Reason: The update.exe file is not fully approved by your personal firewall.

▶ Ensure that the update.exe file is fully approved by your personal firewall.

Otherwise:

▶ Check your settings in the Configuration (expert mode) under General :: Update.

Viruses and malware cannot be moved or deleted.

Reason: The file was loaded by windows and is active.

▶ Update Avira AntiVir Personal.

▶ If you use the operating system Windows XP, deactivate System Restore.

▶ Start the computer in Safe Mode.

▶ Start Avira AntiVir Personal and the Configuration (expert mode).

▶ Choose Scanner :: Scan :: Files :: All files and confirm with **OK**.

▶ Start a scan of all local drives.

▶ Start the computer in Normal Mode.

▶ Carry out a scan in Normal Mode.

▶ If no other viruses or malware have been found, activate System Restore if it is available and to be used.

The status of the tray icon is disabled.

Reason: AntiVir Guard is disabled.

▶ In the Control Center in the section Overview :: Status in theAntiVir Guard panel, click on the **Enable** link.

Reason: AntiVir Guard is blocked by a firewall.

▶ Define a general approval for AntiVir Guard in the configuration of your firewall. AntiVir Guard only works with the address 127.0.0.1 (localhost). An Internet connection is not established.

Otherwise:

▶ Check the startup type of the AntiVir Guard service. If necessary, enable the service: In the taskbar, select "Start | Settings | Control Panel". Start the configuration panel "Services" with a double-click (under Windows 2000 and Windows XP the services applet is located in the sub-directory "Administrative Tools"). Find the entry "Avira AntiVir Guard". "Automatic" must be entered as the startup type and "Started" as the status. If necessary, start the service manually by selecting the relevant line and the button "Start". If an error message appears, please check the event display.

The computer is extremely slow when I perform a data back-up.

Reason: During the back-up procedure, AntiVir Guard scans all files being used by the back-up procedure.

▶ In the configuration (expert mode), choose Guard :: Scan :: Exceptions and enter the names of the backup software processes.

My Firewall reports AntiVir Guard immediately after activation.

Reason: Communication with AntiVir Guardoccurs via the TCP/IP Internet protocol. A firewall monitors all connections via this protocol.

▶ Define a general approval for AntiVir Guard. AntiVir Guard only works with the address 127.0.0.1 (localhost). An Internet connection is not established.

Note
We recommend regularly installing Microsoft updates to close any gaps in security.

8.2 Shortcuts

Keyboard commands - also called shortcuts - offer a fast possibility to navigate, to retrieve individual modules and to start actions through Avira AntiVir Personal.

Below we provide you with an overview of the available keyboard commands in Avira AntiVir Personal. Please find further indications regarding the functionality in the corresponding chapter of the help.

8.2.1 In dialog boxes

Shortcut	**Description**
Ctrl + Tab Ctrl + Page down	Navigation in the Control Center Go to next section.
Ctrl + Shift + Tab Ctrl + Page up	Navigation in the Control Center Go to previous section.
← ↑ → ↓	Navigation in the configuration sections First, use the mouse to set the focus on a configuration section.
Tab	Change to the next option or options group.
Shift + Tab	Change to the previous option or options group.
← ↑ → ↓	Change between the options in a marked drop-down list or between several options in a group of options.
Space	Activate or deactivate a check box, if the active option is a check box.
Alt + underlined letter	Select option or start command.
Alt + ↓ F4	Open selected drop-down list.
Esc	Close selected drop-down list. Cancel command and close dialog.
Enter	Start command for the active option or button.

8.2.2 In the help

Shortcut	**Description**
Alt + Space	Display system menu.
Alt + Tab	Shift between the help and the other opened windows.
Alt + F4	Close help.
Shift + F10	Display context menu of the help.
Ctrl + Tab	Go to next section in the navigation window.
Ctrl + Shift + Tab	Go to previous section in the navigation window.
Page up	Change to the subject, which is displayed above in the contents, in the index or in the list of the search results.
Page down	Change to the subject, which is displayed below the current

	subject in the contents, in the index or in the list of the search results.
Page up Page down	Browse through a subject.

8.2.3 In the Control Center

General

Shortcut	Description
F1	Display help
Alt + F4	Close Control Center
F5	Refresh
F8	Open configuration
F9	Start update

Scan section

Shortcut	Shortcut
F3	Start scan with the selected profile
F4	Create desktop link for the selected profile

Quarantine section

Shortcut	Description
F2	Rescan object
F3	Restore object
F4	Send object
F6	Restore object to...
Return	Properties
Ins	Add file
Del	Delete object

Scheduler section

Shortcut	Description
F2	Edit job
Return	Properties
Ins	Insert new job
Del	Delete job

Reports section

Shortcut	Description
F3	Display report file
F4	Print report file
Return	Display report
Del	Delete report(s)

Events section

Shortcut	Description
F3	Export event(s)
Return	Show event
Del	Delete event(s)

8.3 Windows Security Center

- Windows XP Service Pack 2 or higher -

8.3.1 General

The Windows Security Center checks the status of a computer for important security aspects.

If a problem is detected with one of these important points (e.g. an outdated anti-virus program), the Security Center issues an alert and gives recommendations on how to protect your computer better.

8.3.2 The Windows Security Center and Avira AntiVir Personal

Virus protection software / Protection against malicious software

You may receive the following information from the Windows Security Center with regard to your virus protection.

Virus protection NOT FOUND

Virus protection OUT OF DATE

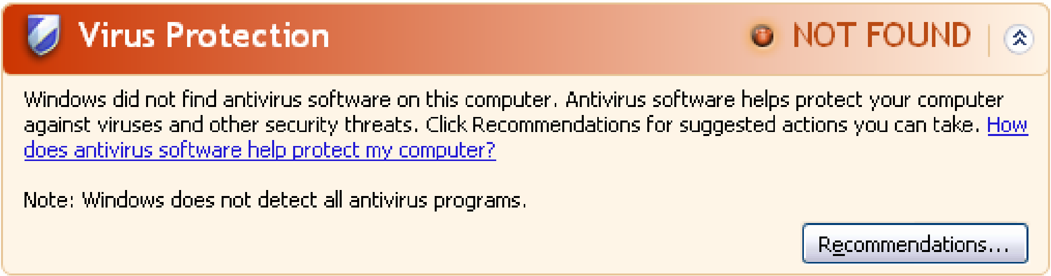
Virus protection ON

Virus protection OFF

Virus protection NOT MONITORED

Virus protection NOT FOUND

This information of the Windows Security Center appears when the Windows Security Center has not found any anti-virus software on your computer.



Virus Protection ● NOT FOUND

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

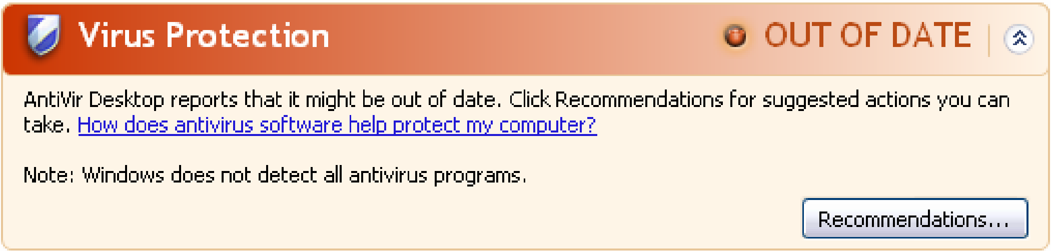
Note: Windows does not detect all antivirus programs.

Note

Install Avira AntiVir Personal on your computer to protect it against viruses and other unwanted programs!

Virus protection OUT OF DATE

If you have already installed Windows XP Service Pack 2 or Windows Vista and then install Avira AntiVir Personal or you install Windows XP Service Pack 2 or Windows Vista on a system on which Avira AntiVir Personal has already been installed, you receive the following message:



Virus Protection ● OUT OF DATE

AntiVir Desktop reports that it might be out of date. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

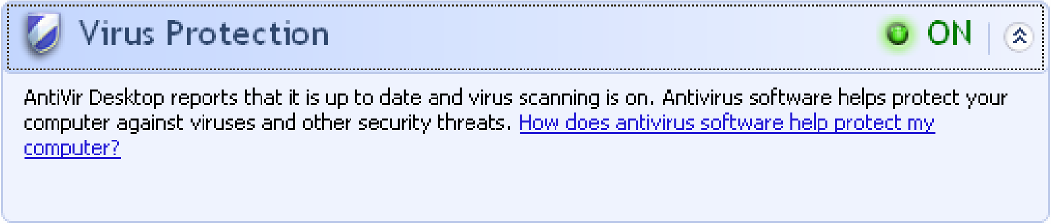
Note: Windows does not detect all antivirus programs.

Note

In order for the Windows Security Center to recognize Avira AntiVir Personal as up to date, an update must be carried out after installation. Update your system by carrying out an Avira AntiVir Personal update.

Virus protection ON

After installation of Avira AntiVir Personal and a subsequent update, you receive the following message:



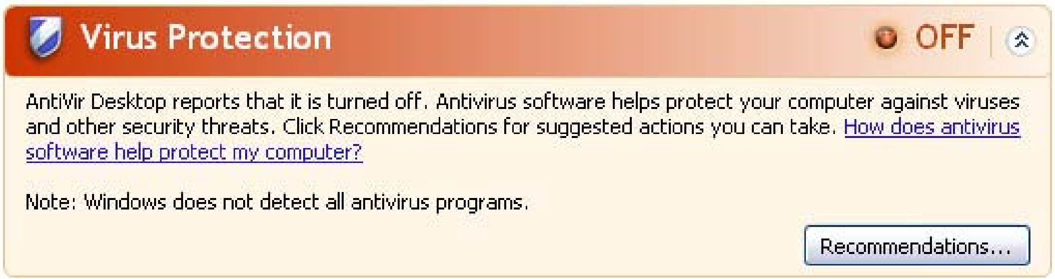
Virus Protection ● ON

AntiVir Desktop reports that it is up to date and virus scanning is on. Antivirus software helps protect your computer against viruses and other security threats. How does antivirus software help protect my computer?

Avira AntiVir Personal is now up to date and the AntiVir Guard is enabled.

Virus protection OFF

You receive the following message if you disable the AntiVir Guard or stop the Guard service.



Virus Protection ● OFF

AntiVir Desktop reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

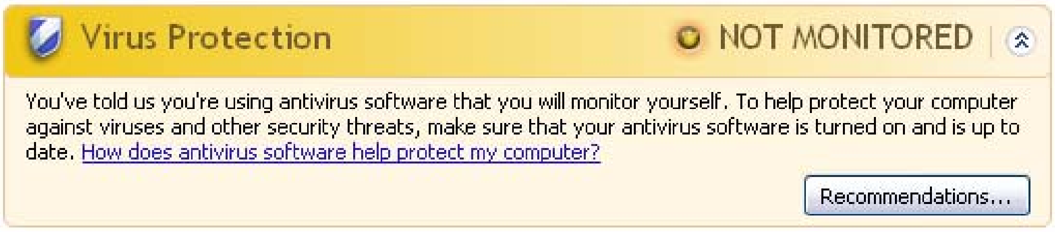
Note: Windows does not detect all antivirus programs.

Note
You can enable or disabled AntiVir Guard in the Overview :: Status section of theAvira AntiVir Personal Control Center . You can also see that the AntiVir Guard is enabled if the red umbrella in your taskbar is open.

Virus protection NOT MONITORED

If you receive the following message from the Windows Security Center, you have decided that you want to monitor your anti-virus software yourself.

Note
This function is not supported by Windows Vista.



Virus Protection ● NOT MONITORED

You've told us you're using antivirus software that you will monitor yourself. To help protect your computer against viruses and other security threats, make sure that your antivirus software is turned on and is up to date. How does antivirus software help protect my computer?

Note
The Windows Security Center is supported by Avira AntiVir Personal. You can enable this option at any time via the button "Recommendations...".

Note
Even if you have installed Windows XP Service Pack 2 or Windows Vista, you still require a virus protection solution, e.g. Avira AntiVir Personal. Although Windows XP Service Pack 2 monitors your anti-virus software, it does not contain any anti-virus functions itself. Therefore you would not be protected against viruses and other malware without an additional anti-virus solution!

9 Viruses and more

9.1 Extended threat categories

Dialers (DIALERS)

Certain services available in the Internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the Internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask directly your telephone provider to block this number range to be immediately protected against undesired dialers (0190/0900 dialers).

Avira AntiVir Personal can detect the familiar dialers by default.

If the option **Dialers** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if a dialer is detected. You can now simply delete the potentially unwanted 0190/0900 dialer. However, if it is a wanted dial-up program, you can declare it an exceptional file and this file is then no longer scanned in future.

Games (GAMES)

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the Internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Avira AntiVir Personal detects computer games. If the **Games** option is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects a game. The game is now over in the truest sense of the word, because you can simply delete it.

Jokes (JOKES)

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Thanks to the extension of its scanning and identification routines, Avira AntiVir Personal is able to detect joke programs and eliminate them as unwanted programs if required. If the option **Jokes** is enabled with a check mark in the configuration under Extended threat categories, a corresponding alert is issued if a joke program is detected.

Security Privacy Risk (SPR)

Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.

Avira AntiVir Personal detects "Security Privacy Risk" software. If the option **Security Privacy Risk** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects such software.

Backdoor Clients (BDC)

In order to steal data or manipulate computers, a backdoor server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the Internet or a network.

Avira AntiVir Personal detects "backdoor control software". If the option **Backdoor Clients** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects such software.

Adware/Spyware (ADSPY)

"Software that displays advertising or software that sends the user&apos;s personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted."

Avira AntiVir Personal detects "Adware/Spyware". If the option **Adware/Spyware** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects such software.

Unusual Runtime Compression Tools (PCK)

Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

Avira AntiVir Personal detects "Unusual runtime Compression Tools". If the option **Unusual runtime Compression Tools** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects such packers.

Double Extension Files (HEUR-DBLEXT)

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Avira AntiVir Personal detects "Double Extension Files". If the option **Double Extension files** (HEUR-DBLEXT) is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects such files.

Phishing

Phishing, also known as *brand spoofing* is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.
When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

Avira AntiVir Personal detects "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira AntiVir Personal detects such behavior.

Application (APPL)

The term APPL refers to an application which may involve a risk when used or is of dubious origin.

Avira AntiVir Personal detects "Application (APPL)". If the option **Application (APPL)** is enabled with a check mark in the configuration under Extended threat categories , you receive a relevant alert if Avira AntiVir Personal detects such behavior.

9.2 Viruses and other malware

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Backdoors

A backdoor can gain access to a computer by circumventing computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help, but are mainly used to install further computer viruses or worms on the relevant system. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Boot viruses

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more&ldots;

Bot-Net

A bot net is defined as a remote network of PCs (on the Internet), which is composed of bots that communicate with each other. A Bot-Net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-Nets serve various purposes, including Denial-of-service attacks etc., partly without the affected PC user's knowledge. The main potential of Bot-Nets is that the networks can achieve dimensions on thousands of computers and its bandwidth sum bursts most conventional Internet accesses.

Exploit

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. A form of an exploit for example are attacks from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

Hoaxes

For several years, Internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread per email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

Honeypot

A honeypot is a service (program or server) installed in a network. It has the function to monitor a network and to protocol attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a Honeypot, it is logged and an alert is triggered.

Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses do consequently not attack executable files but they do attack the documents of the corresponding host-application.

Pharming

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

Phishing

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

Polymorph viruses

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

Program viruses

A computer virus is a program that is capable to attach itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits his virulent code. The program execution of the host itself is not changed as a rule.

Rootkit

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

Script viruses and worms

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms can consequently not form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

Spyware

Spyware are so-called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

Trojan horses (short Trojans)

Trojans are pretty common nowadays. We are talking about programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

Zombie

A Zombie-PC is a computer that is infected with malware programs and enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

10 Info and Service

This chapter contains information on how to contact us.

see Chapter Contact address

see Chapter Technical support

see Chapter Suspicious files

see Chapter Report false positives

10.1 Contact address

If you have any questions or requests concerning the Avira AntiVir Personal product range, we will be pleased to help you. You will find our contact addresses in the Control Center under Help :: About Avira AntiVir Personal.

10.2 Technical Support

Avira AntiVir Personal support provides reliable assistance in answering your questions or solving a technical problem.

All necessary information on our comprehensive support service can be obtained from our website http://www.avira.com/personal-support.

All necessary information on our comprehensive support service can be obtained from our website http://www.avira.com/personal-support.

- **Version information**. This can be found on the program interface under the menu item Help :: About AntiVir Personal :: Version information.
- **Operating system version** and any Service Packs installed.
- **Installed software packages**, e.g. anti-virus software of other vendors.
- **Exact messages** of the program or of the report file.

10.3 Suspicious file

Viruses that may not yet be detected or removed by our products or suspect files can be sent to us. We provide you with several ways of doing this.

- Identify the file in the Quarantine Manager of the Control Center and select the item Send file via the context menu or the corresponding button.

- Send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus-personal@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

10.4 Reporting false positives

If you believe that Avira AntiVir Personal reports something about a file that is most likely "clean", send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus-personal@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

11 Reference: Configuration options

The configuration reference documents all configuration options available in Avira AntiVir Personal.

11.1 Scanner

The Scanner section of the Configuration is responsible for the configuration of the on-demand scan.

11.1.1 Scan

Here you define the basic behavior of the scan routine for an on-demand scan. If you select certain directories to be scanned with an on-demand scan, depending on the configuration the Scanner scans:

- with a certain scanning power (priority),
- also boot sectors and main memory,
- certain or all boot sectors and the main memory,
- all or selected files in the directory.

Files

The Scanner can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and file extension. The filter is not used.

Note
If All files is enabled, the button File extensions cannot be selected.

Smart Extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by Avira AntiVir Personal. This means that Avira AntiVir Personal decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since not only on the basis of the file extension is scanned. This setting is activated by default and is recommended.

Note
If Smart Extensions is enabled, the button File extensions cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button File extension.

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the button File extensions.

File extensions

With the aid of this button, a dialog window is opened in which all file extensions are displayed that are scanned in **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the default list may vary from version to version.

Additional settings

Scan boot sectors of selected drives

If this option is enabled, the Scanner only scans the boot sectors of the drives selected for the on-demand scan. This option is enabled as the default setting.

Scan master boot sectors

If this option is enabled, the Scanner scans the master boot sectors of the hard disk(s) used in the system.

Ignore offline files

If this option is enabled, the direct scan ignores so-called offline files completely during a scan. This means that these files are not scanned for viruses and unwanted programs. Offline files are files that were physically moved by a so-called Hierarchical Storage Management System (HSMS) from the hard disk onto a tape, for example. This option is enabled as the default setting.

Integrity checking of system files

When this option is enabled, the most important Windows system files are subjected to a particularly secure check for changes by malware during every on-demand scan. If an amended file is detected, this is reported as suspect. This function uses a lot of computer capacity. That is why the option is disabled as the default setting.

Important
This option is only available with Windows Vista and higher.

Note
This option should not be used if you are using third-party tools that modify system files and adapt the boot or start screen to your own requirements. Examples of such tools are skinpacks, TuneUp utilities or Vista Customization.

Optimized scan

When the option is enabled, the processor capacity is optimally utilized during a Scanner scan. For performance reasons, an optimized scan is only logged on standard level.

Note
This option is only available on multi-processor systems.

Follow symbolic links

If this option is enabled, Scanner performs a scan that follows all symbolic links in the scan profile or selected directory and scans the linked files for viruses and malware. This option is not supported by Windows 2000 and has been deactivated.

Important
The option does not include any shortcuts, but refers exclusively to symbolic links (generated by mklink.exe) or Junction Points (generated by junction.exe) which are transparent in the file system.

Search for Rootkits before scan

If this option is enabled and a scan is started, the scanner scans the Windows system directory for active rootkits in a so-called shortcut. This process does not scan your computer for active rootkits as comprehensively as the scan profile **Scan for rootkits**, but it is significantly quicker to perform.

Important
The rootkit scan is not available for Windows XP 64 bit !

Scan Registry

If this option is enabled, the Registry is scanned for references to malware.

Scan process

Allow stopping the scanner

If this option is enabled, the scan for viruses or unwanted programs can be terminated at any time with the button Stop in the "Luke Filewalker"window. If you have disabled this setting, the Stop button in the "Luke Filewalker"window has a gray background. Premature ending of a scan process is thus not possible! This option is enabled as the default setting.

Scanner priority

With the on-demand scan, the Scanner distinguishes between priority levels. This is only effective if several processes are running simultaneously on the workstation. The selection affects the scanning speed.

Low

The Scanner is only allocated processor time by the operating system if no other process requires computation time, i.e. as long as only the Scanner is running, the speed is maximum. All in all, work with other programs is optimal: The computer responds more quickly if other programs require computation time while the Scanner continues running in the background. This setting is activated by default and is recommended.

Medium

The Scanner is executed with normal priority. All processes are allocated the same amount of processor time by the operating system. Under certain circumstances, work with other applications may be affected.

High

The Scanner has the highest priority. Simultaneous work with other applications is almost impossible. However, the Scanner completes its scan at maximum speed.

11.1.1.1. Action for concerning files

Action for concerning files

You can define the actions to be carried out by Scanner when a virus or unwanted program is detected.

Interactive

If this option is enabled, the results of the Scanner scan are displayed in a dialog box. When carrying out a scan with the Scanner, you will receive an alert with a list of the affected files at the end of the scan. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the Scanner.

Note
The action Move to quarantine is pre-selected by default in the Scanner notification. Further actions can be selected via a context menu.

Click here for more information.

Automatic

If this option is enabled, then no dialog box for selecting an action appears following the detection of a virus or unwanted program. The Scanner reacts according to the settings you define in this section.

Backup to quarantine

If this option is enabled, the Scanner creates a backup copy before carrying out the requested primary or secondary action. The back-up copy is saved in quarantine, where the file can be restored if it is of informative value. You can also send the backup copy to the Avira Malware Research Center for further investigation.

Primary action

Primary action is the action carried out when the Scanner finds a virus or an unwanted program. If the option **repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.

Note
The option Secondary action can only be selected if the setting **repair** was selected under Primary action.

repair

If this option is enabled, the Scanner repairs affected files automatically. If the Scanner cannot repair an affected file, it carries out the action selected under Secondary action.

Note
An automatic repair is recommended, but means that the Scanner modifies files on the workstation.

delete

If this option is enabled, the file is deleted.

rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Secondary action

The option **Secondary action** can only be selected if the setting **Repair** was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

delete

If this option is enabled, the file is deleted.

rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Note
If you have selected **Delete**or as the primary or secondary action, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

When scanning archives, the Scanner uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again.

Scan archives

If this option is enabled, the selected archives in the archive list are scanned. This option is enabled as the default setting.

All archive types

If this option is enabled, all archive types in the archive list are selected and scanned.

Smart Extensions

If this option is enabled, the Scanner detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. However, for this every file must be opened - which reduces the scanning speed. Example: if a *.zip archive has the file extension *.xyz, the Scanner also unpacks this archive and scans it. This option is enabled as the default setting.

Note
Only those archive types are supported, which are marked in the archive list.

Limit recursion depth

Unpacking and scanning recursive archives can require a great deal of computer time and resources. If this option is enabled, you limit the depth of the scan in multi-packed archives to a certain number of packing levels (maximum recursion depth). This saves time and computer resources.

Note
In order to find a virus or an unwanted program in an archive, the Scanner must scan up to the recursion level in which the virus or the unwanted program is located.

Maximum recursion depth

In order to enter the maximum recursion depth, the option Limit recursion depth must be enabled.
You can either enter the requested recursion depth directly or by means of the right arrow key on the entry field. The permitted values are 1 to 99. The standard value is 20 which is recommended.

Default values

The button restores the pre-defined values for scanning archives.

Archives

In this display area you can set which archives the Scanner should scan. For this, you must select the relevant entries.

11.1.1.2. Exceptions

File objects to be omitted for the scanner

The list in this window contains files and paths that should not be included by the Scanner in the scan for viruses or unwanted programs.

Please enter as few exceptions as possible here and really only files that, for whatever reason, should not be included in a normal scan. We recommend that you always scan these files for viruses or unwanted programs before they are included in this list!

Note
The entries on the list must not result in more than 6000 characters in total.

Warning
These files are not included in a scan!

Note
The files included in this list are entered in the report file. Please check the report file from time to time for unscanned files, as perhaps the reason you excluded a file here no longer exists. In this case you should remove the name of this file from this list again.

Input box

In this input box you can enter the name of the file object that is not included in the on-demand scan. No file object is entered as the default setting.

[...]

The button opens a window in which you can select the required file or the required path.
When you have entered a file name with its complete path, only this file is not scanned for infection. If you have entered a file name without a path, all files with this name (irrespective of the path or drive) are not scanned.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Note

If you add a complete partition to the list of the file objects, only those files which are saved directly under the partition will be excluded from the scan, which does not apply for files in sub-directories on the corresponding partition:
Example: File object to be skipped: `D:\ = D:\file.txt` will be excluded from the scan of the Scanner, `D:\folder\file.txt` will not be excluded from the scan.

11.1.1.3. Heuristic

This configuration section contains the settings for the heuristic of the Avira AntiVir Personal search engine.

Avira AntiVir Personal contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Avira AntiVir Personal contains a highly powerful macro virus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

enable AHeAD

Avira AntiVir Personal contains a very powerful heuristic in the form of AntiVir AheAD technology, which can also detect unknown (new) malware. If this option is activated, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira AntiVir Personal detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This setting is activated by default if you have selected the use of this heuristic.

High detection level

If this option is enabled, Avira AntiVir Personal detects much more unknown malware, however false positives can also be expected.

11.1.2 Report

The Scanner has a comprehensive reporting function. You thus obtain precise information on the results of an on-demand scan. The report file contains all entries of the system as well as alerts and messages of the on-demand scan.

Note
To enable you to establish what actions the Scanner has carried out when viruses or unwanted programs have been detected, a report file should always be created.

Reporting

Off

If this option is enabled, the Scanner does not report the actions and results of the on-demand scan.

Default

When this option is activated, the Scanner logs the names of the files concerned with their path. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

Advanced

When this option is activated, the Scanner logs alerts and tips in addition to the default information.

Complete

When this option is activated, the Scanner also logs all scanned files. In addition, all files involved as well as alerts and tips are included in the report file.

Note
If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

11.2 Guard

The Guard section of the configuration is responsible for the configuration of the on-access scan.

11.2.1 Scan

You will normally want to monitor your system constantly. To this end, use the Guard (= on-access scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

Scan mode

Here the time for scanning of a file is defined.

Scan when reading

If this option is enabled, the Guard scans the files before they are read or executed by the application or the operating system.

Scan when writing

If this option is enabled, the Guard scans a file when writing. You can only access the file again after this process has been completed.

Scan when reading and writing

If this option is enabled, the Guard scans files before opening, reading and executing and after writing. This option is enabled as the default setting and is recommended.

Files

The Guard can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files, irrespective of their content and their file extension, are scanned for viruses or unwanted programs, i.e. the filter is not used.

Note
If All files is enabled, the button File extensions cannot be selected.

Smart Extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by Avira AntiVir Personal. This means that Avira AntiVir Personal decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since not only on the basis of the file extension is scanned.

Note
If Smart Extensions is enabled, the button File extensions cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button File extension. This setting is activated by default and is recommended.

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the button File extensions.

File extensions

With the aid of this button, a dialog window is opened in which all file extensions are displayed that are scanned in **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the file extension list may vary from version to version.

Archives

Scan archives

If this option is enabled, then archives will be scanned. Compressed files are scanned, then decompressed and scanned again. This option is deactivated by default. The archive scan is restricted by the recursion depth, the number of files to be scanned and the archive size. You can set the maximum recursion depth, the number of files to be scanned and the maximum archive size.

Note
This option is deactivated by default, since the process puts heavy demands on the computer's performance. It is generally recommended that archives be checked using an on-demand scan.

Maximum recursion depth

When scanning archives, the Guard uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. You can define the recursion depth. The default value for the recursion depth is 1 and is recommended: all archives that are directly located in the main archive are unpacked and scanned.

Maximum number of files

When scanning archives, you can restrict the scan to a maximum number of files in the archive. The default value for the maximum number of files to be scanned is 10 and is recommended.

Maximum size (KB)

When scanning archives, you can restrict the scan to a maximum archive size to be unpacked. The standard value of 1000KB is recommended.

11.2.1.1. Action for concerning files

Notifications

Use event log

When this option is enabled, an entry is added to the event log for every detection. The administrator can identify detections and react accordingly. This option is enabled as the default setting.

Autostart

Block autostart function

When this option is enabled, the execution of the Windows Autostart function is blocked on all connected drives, including USB sticks, CD and DVD drives and network drives. With the Windows Autostart function, files on data media or network drives are read immediately on loading or connection, and files can therefore be started and copied automatically. This functionality however carries with it a high security risk, as malware and unwanted programs can be installed with the automatic start. The Autostart function is especially critical for USB sticks as data on a stick can be changed at any time.

Exclude CDs and DVDs

When this option is enabled, the Autostart function is permitted on CD and DVD drives.

Warning
Only disable the Autostart function for CD and DVD drives if you are sure you are only using trusted data media.

11.2.1.2. Exceptions

With these options you can configure exception objects for the Guard (on-access scan). The relevant objects are then not included in the on-access scan. The Guard can ignore file accesses to these objects during the on-access scan via the list of processes to be omitted. This is useful, for example, with databases or back-up solutions.

Processes to be omitted by the Guard

All file accesses of processes in this list are excluded from monitoring by Guard.

Input box

In this field, enter the name of the process that is to be ignored by the real-time scan. No process is entered as the default setting.

Note
You can enter up to 128 processes.

Note
The entries on the list must not result in more than 6000 characters in total.

Warning:
The specified path and file name of the process should contain a maximum of 255 characters.

Warning
Please note that all file accesses by processes recorded in the list are excluded from the scan for viruses and unwanted programs! The Windows Explorer and the operating system itself cannot be excluded. A corresponding entry in the list is ignored.

...

The button opens a window in which you can select an executable file.

Processes

The**Processes** button opens the *Process selection* window in which the running processes are displayed.

Add

With this button, you can add the process entered in the input box to the display window.

Delete

With this button you can delete a selected process from the display window.

File objects to be omitted by the Guard

All file accesses to objects in this list are excluded from monitoring by the Guard.

Input box

In this box you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.

Note
The entries in the list must have no more than 6000 characters in total.

Note
For each drive you can specify a maximum of 20 exceptions by entering the complete path (starting with the drive letter).
E.g.: C:\Program Files\Application\Name.log

The maximum number of exceptions without a complete path is 64.
For example: *.log

...

The button opens a window in which you can select the file object to be excluded.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

With this button you can delete a selected file object from the display window.

Please observe the following points:

- The file name can only contain the wildcards * (any number of characters) and ? (a single character).
- Directory names must end with a backslash \, otherwise a file name is assumed.
- The list is processed from top to bottom.
- Individual file extensions can also be excluded (inclusive wildcards).
- If a directory is excluded, all its sub-directories are automatically also excluded.
- The longer the list is, the more processor time is required for processing the list for each access. Therefore, keep the list as short as possible.
- In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.

Note
A file name that contains wildcards may not be terminated with a backslash.

For example:

```
C:\Program Files\Application\applic*.exe\
```

This entry is not valid and not treated as an exception!

Note
In case of dynamic drives which are mounted as a directory on another drive, the alias of the operating system for the integrated drive in the list of the exceptions has to be used: e.g. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
If you use the mount point itself, for example, C:\DynDrive, the dynamic drive will be scanned nonetheless. You can determine the alias of the operating system to be used from the Guard report file.

Note
You can locate the path Guard uses to scan for infected files in the Guard report file. Indicate exactly the same path in the list of exceptions. Proceed as follows: set the protocol function of Guard to **Complete** in the configuration under Guard :: Report. Now access the files, folders, mounted drives with the activated Guard. You can now read the path to be used from the Guard report file. The report file can be accessed in the Control Center under Local protection :: Guard.

Examples:

```
C:
C:\
C:\*.*
C:\*
```

```
*.exe
*.xl?
*.*
C:\Program Files\Application\application.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\applic*
C:\Program Files\Application\applic?????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Application\*.mdb
```

11.2.1.3. Heuristic

This configuration section contains the settings for the heuristic of the Avira AntiVir Personal search engine.

Avira AntiVir Personal contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Avira AntiVir Personal contains a highly powerful macro virus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

enable AHeAD

Avira AntiVir Personal contains a very powerful heuristic in the form of AntiVir AheAD technology, which can also detect unknown (new) malware. If this option is activated, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira AntiVir Personal detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This setting is activated by default if you have selected the use of this heuristic.

High detection level

If this option is enabled, Avira AntiVir Personal identifies far more unknown malware, but you must also accept that there are likely to be false positives.

11.2.2 Report

Guard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Guard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then Guard does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, Guard records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Advanced

If this option is enabled, Guard logs less important information to the report file as well.

Complete

If this option is enabled, Guard logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: 1 to 100 MB. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Backup report file before shortening

If this option is enabled, the report file is backed up before shortening.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

11.3 Update

In the *Update* section you can configure the automatic receiving of updates. You can specify various update intervals and activate or deactivate automatic updating.

Automatic update

Activate

If this option is enabled, automatic updates are performed for the enabled events at the interval specified.

Automatic update every n days / hours / minutes

In this box you can specify the interval at which the automatic update is carried out. To change the update interval, highlight one of the time options in the box and change it using the arrow key to the right of the input box.

Repeat job if the time has already expired

If this option is enabled, past update jobs are carried out that could not be carried out at the time specified, for example because the computer was switched off.

11.3.1 Product update

Under **Product update**, configure how product updates or the notification of available product updates are handled.

Product updates

Download and automatically install product updates

If this option is enabled, product updates are downloaded and automatically installed by the Update component as soon as they become available. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Download product updates. If a restart is necessary, install the update after the system restart, otherwise install it immediately.

If this option is enabled, product updates will be downloaded as soon as they become available. If no restart is necessary, the update is installed automatically after the update file is downloaded. If a product update requires you to restart your computer, it will be executed at the next user-controlled system reboot and not immediately after the download of the update file. This has the advantage that the restart is not carried out while users are working at their computers. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Notification when new product updates are available

If this option is enabled, you will be notified by email when new product updates become available. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server. You will receive notifications via a desktop popup window and via an alert from the Updater in the Control Centre under Overview::Events.

Notify again after n day(s)

If the product update was not installed after the initial notification, enter in this box the number of days that are to elapse before you are again notified that product updates are available.

Do not download product updates

If this option is enabled, no automatic product updates or notifications of available product updates by the Updater are carried out. Updates to the virus definition file and search engine are carried out independently of this setting.

Important
An update of the virus definition file and of the search engine is carried out during every update process independent of the settings for the product update (see chapter Updates).

11.3.2 Restart settings

When a product update is carried out by AntiVir Personal, you may have to restart your computer system. If you have selected automatic product updates under General::Update::Product update , you can choose between the different restart notification and restart cancellation options under **Restart settings**.

Note
Note that your restart settings allow you to choose between two options for executing a product update requiring a computer restart in the configuration under General::Update::Product update.

Automatic execution of the product update with the required computer restart when update is available: the update and the restart are carried out while users are working on their computers. If you have enabled this option, it may be useful to select restart routines with a cancel option or reminder function.

Execution of the product update where a computer restart is required after the next system reboot: the update and the restart are carried out after users have started up their computers and logged in. Automatic restart routines are recommended for this option..

Restart settings

Restart the computer after n seconds

If this option is enabled, the necessary restart is carried out **automatically** after a product update has been executed at the interval specified. A countdown message appears with no option for canceling the computer restart..

Reminder message for restart every n seconds

If this option is enabled, the necessary restart is **not** carried out automatically after a product update has been executed. At the interval specified, you will receive restart notifications without cancel options. These notifications let you confirm the computer restart or select **Remind me again** .

Query whether computer should be restarted

If this option is enabled, the necessary restart is **not** carried out automatically after a product update has been executed. You will receive one message in which you can confirm the restart or cancel the restart routine.

Restart computer without query

If this option is enabled, the necessary restart is carried out **automatically** after a product update has been executed. You will not receive any notification.

11.3.3 Web server

The update can be performed directly via a web server on the Internet.

Web server connection

Use existing connection (network)

This setting is displayed if your connection is used via a network.

Use the following connection:

This setting is displayed if you define your connection individually.

The Updater automatically detects which connection options are available. Connection options which are not available are grayed out and cannot be activated. A dial-up connection can be established manually via a phone book entry in Windows, for example.

- **User:** Enter the user name of the selected account.
- **Password:** Enter the password for this account. For security, the actual characters you type in this space are replaced by asterisks (*).

Note
If you have forgotten an existing Internet account name or password, contact your Internet Service Provider.

Note
The automatic dial-up of the updater through so-called dial-up tools (e.g. SmartSurfer, Oleco, ...) is currently not available in Avira AntiVir Personal.

Terminate a dial-up connection that was set up for the update

If this option is enabled, the RDT connection made for the update is automatically interrupted again as soon as the download has been successfully carried out.

Note
This option is not available under Vista. Under Vista the dial-up connection opened for the update is always terminated as soon as the download has been carried out.

11.3.3.1. Proxy

Proxy server

Do not use a proxy server

If this option is enabled, your connection to the web server is not carried out via a proxy server.

Use Windows system settings

When the option is enabled, the current Windows system settings are used for the connection to the web server via a proxy server.

Use the following proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

Address

Please enter the URL or the IP address of the proxy server you should use to connect to the web server.

Port

Please enter the port number of the proxy server you should use to connect to the web server.

Login name

Enter your login name on the proxy server here.

Login password

Enter the relevant password for logging in on the proxy server here. For security, the actual characters you type in this space are replaced by asterisks (*).

Examples:

Address:	proyx.domain.com	Port:	8080
Address:	192.168.1.100	Port:	3128

11.4 General

11.4.1 Extended threat categories

Selection of extended threat categories

Avira AntiVir Personal protects you against computer viruses.

In addition, you can scan according to the following extended threat categories.

- Backdoor Clients (BDC)
- Dialer (DIALER)
- Games (GAMES)
- Jokes (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Unusual runtime packers (PCK)
- Double Extension Files (HEUR-DBLEXT)
- Phishing
- Application (APPL)

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

Select all

If this option is enabled, all types are enabled.

Default values

This button restores the predefined default values.

Note
If a type is disabled, files recognized as being of the relevant program type are no longer indicated. No entry is made in the report file.

11.4.2 Security

Update

Alert if last update older than n day(s)

In this box you can enter the maximum number of days allowed to have passed since the last update of Avira AntiVir Personal. If this number of days has passed, a red icon is displayed for the update status under Status in the Control Center.

Show notice if the virus definition file is out of date

If this option is enabled, you will obtain an alert message if the virus definition file is not up-to date. With the help of the alert option, you can configure the temporal interval for an alert message if the last update is older than n day(s).

Product protection

Protect processes from unwanted termination

If this option is enabled, all AntiVir Personal processes are protected against unwanted termination by viruses and malware or against 'uncontrolled' termination by a user e.g. via Task-Manager. This option is enabled as the default setting.

Advanced password protection

If this option is enabled, all AntiVir Personal processes are protected with advanced options from unwanted termination. Advanced password protection requires considerably more computer resources than simple password protection . That is why the option is disabled as the default setting. To enable this option, you have to restart your computer.

Important
Password protection is not available for Windows XP 64 Bit !

Warning
If process protection is enabled, interaction problems can occur with other software products. Disable process protection in these cases.

Protect files and registry entries from manipulation

If this option is enabled, all registry entries of AntiVir Personal and all program files (binary and configuration files) are protected from manipulation. Protection against manipulation entails preventing write, delete and, in some cases, read access to the registry entries or program files by users or external programs. To enable this option, you have to restart your computer.

Note
When this option is activated, changes can only be made to the configuration, including changes to scan or update requests, can only be made by means of the user interface.

Important
Protection for files and registration entries is not available for Windows XP 64 Bit !

11.4.3 WMI

Support for Windows Management Instrumentation

Windows Management Instrumentation is a basic Windows administration technique that uses script and programming languages to allow read and write access, both local and remote, to settings on Windows systems. AntiVir Personal supports WMI and provides data (status information, statistical data, reports, planned requests, etc.) as well as events at an interface. WMI enables you to download operating data from AntiVir Personal .

Enable WMI support

When this option is enabled, you can download operating data from AntiVir Personal via WMI.

11.4.4 Directories

Temporary path

In this input box, enter the path where Avira AntiVir Personal will store its temporary files.

Use default system settings

If this option is enabled, the settings of the system are used for handling temporary files.

Note
You can see where your system saves temporary files - for example with Windows XP - under: Start | Settings | Control Panel | System | Tab "Advanced" | Button "Environment Variables". The temporary variables (TEMP, TMP) for the currently registered user and for system variables (TEMP, TMP) are shown here with their relevant values.

Use following directory

If this option is enabled, the path displayed in the input box is used.

...

The button opens a window in which you can select the required temporary path.

Default

The button restores the pre-defined directory for the temporary path.

11.4.5 Events

Limit size of event database

Limit maximum number of events to n entries

If this option is enabled, the maximum number of events listed in the event database can be limited to a certain size; possible values: 100 to 10 000 entries. If the number of entered entries is exceeded, the oldest entries are deleted.

Delete events older than n day(s)

If this option is enabled, events listed in the event database are deleted after a certain period of time; possible values: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

Do not limit size of event database (delete events manually)

When this option has been activated, the size of the event database is not limited. However, a maximum of 20,000 entries are displayed in the program interface under Events.

11.4.6 Limit reports

Limit number of reports

Limit the number to n units

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

Delete all reports more than n day(s) old

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are: 1 to 90 days. This option is enabled by default with a value of 30 days.

Do not limit number of reports (manually delete reports)

If this option is enabled, the number of reports is not restricted.

11.4.7 Acoustic alerts

Acoustic alert

When a virus or malware is detected by the Scanner or Guard an acoustic alert is sounded in interactive action mode. You can now choose to activate or deactivate the acoustic alert and select an alternative wave file for the alert.

Note
The action mode of the Scanner is set in the configuration under Scanner::Scan::Action for concerning files.

No warning

When this option is activated, there is no acoustic alert when a virus is detected by the Scanner or Guard.

Use PC speakers (only in interactive mode)

If this option is enabled, there is an acoustic alert with the default signal when a virus is detected by the Scanner or Guard. The acoustic alert is sounded on the PC’s internal speaker.

Use the following Wave file (interactive mode only)

If this option is enabled, there is an acoustic alert with the selected Wave file when a virus is detected by the Scanner or Guard. The selected Wave file is played over a connected external speaker.

Wave file

In this input box you can enter the name and the associated path of an audio file of your choice. The default acoustic signal of AntiVir Personal is entered as standard.

The button opens a window in which you can select the required file with the aid of the file explorer.

Test

This button is used to test the selected wave file.

11.4.8 Warnings

AntiVir Personal generates so-called slide-ups, desktop notifications for specific events, which give information on successful or failed program sequences, such as updates. In *Warnings* you can enable or disable the notifications for specific events..

With desktop notifications, you have the option of disabling the notification directly in the slide-up. You can reverse the disabling of the notification in *Warnings*.

Warnings

on dial-up connections used

If this option is enabled, you will receive a desktop notification alert if a dialer creates a dial-up connection on your computer via the telephone or ISDN network. There is a danger that the connection may have been created by an unknown and unwanted dialer and that the connection may be chargeable. (see Viruses and more::Extended threat categories: Dialer).

on successfully updated files

If this option is enabled, you will receive a desktop notification whenever an update has been successfully performed and files updated.

on failed update

If this option is enabled, you will receive a desktop notification whenever an update fails: No connection to the download server could be created or the update files could not be installed.

that no update is necessary

If this option is enabled, you will receive a desktop notification whenever an update is started but installation of the files is not necessary as your program is up to date.

that you are logged on with administrator rights

If this option is enabled, when you log on to your computer, you will receive an alert if your user account includes administrator rights. For security reasons, it is recommended that you work with restricted user rights. By restricting the user rights with which you work on your computer, you prevent the automatic installation of unwanted programs and the unauthorized changing of system settings.

Avira AntiVir Personal – Free Antivirus

www.avira.com

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com

This manual was created with great care. However, errors in design and contents cannot be excluded.
The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q1-2010

AVIRA®